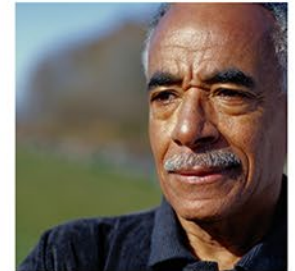


Information Security and Privacy Training for New Employees



Office of Information Security
Field Security Service

Know your Information System Security Officers & Privacy Officers

Information System Security Officers – Email Group VHAPTH ISO



Brian Kohler



Steve Changet



Terry Dziadik

Privacy Officers – Email Group VHAPTH Privacy



Jeffrey Adamson



Lisa Hoss

VA Privacy and Information Security Training Requirements

- You will be required to complete the following training every 365 days in the Talent Management System (TMS) :
 - VA Privacy and Information Security Awareness and Rules of Behavior (all staff)
 - Privacy and HIPAA Focused Training (staff who have access to PHI)
- If you are delinquent, your computer access will be disabled.
- You will get reminders if your TMS profile is correct.
- You are responsible for knowing and following the National Rules of Behavior.

The screenshot displays the VALU TMS interface. At the top, there are logos for the Department of Veterans Affairs, VALU (VA Learning University), and the TMS. Below the logos are navigation tabs for 'Home' and 'Admin'. The main section is titled 'To-Do List' and contains a search bar labeled 'Search Learning Plan' and a 'Show:' dropdown menu set to 'Everything'. The list shows two training items:

- VA Privacy and Information Security Awareness and Rules of Behavior**
Due by 10/13/2015 | Required | Assigned by System AP | Originated From Curriculum
Department of Veterans Affairs 10176
VA Privacy and Information Security Awareness and Rules of Behavior (ROB) provides information security and privacy training important to everyone who...[more](#)
Available
Buttons: Start Course, View Details
- Privacy and HIPAA Focused Training**
Due by 1/20/2016 | Required | Assigned by System AP | Originated From Curriculum
Department of Veterans Affairs 10203
This course is available in two formats, web-based and text-PDF. These materials have been updated for FY2015. Either of these course versions must be...[more](#)
Available
Buttons: Start Course, View Details

PIV cards

- Should be displayed at all times (exceptions for certain staff)
- Unlock computer
 - 6 digit PIN lasts for the life of the card
 - Removal of the card will not lock the computer.
 - Do not leave the PIV card unattended.
- Encrypt Email
 - Certificates must be installed
 - Instructions found on the ISO SharePoint page
- Lost or stolen PIV cards should be reported to your supervisor, ISSO, AND Police IMMEDIATELY.



Functional Categories

- As a part of assigned job duties, some employees will have access to the VAs electronic medical record system. This does not mean you have a right nor need to know to any record that is available. Accessing a record because you are curious is not authorized.
- All VHA personnel must use, disclose, or request protected health information to the minimum amount necessary required to perform their specific job function and to accomplish the intended purpose of the use, disclosure, or request. Not everyone has a need to know, including co-workers.
- All VHA personnel are classified into at least one designated functional category. Staff must not access information that exceeds the limits of protected health information for their functional category. VHA personnel should only access PHI needed to perform their official job function even if the functional category to which they have been assigned allows for greater access. **You will sign an acknowledgement of this classification initially and each year thereafter.**
- The VA National Rules of Behavior that are signed by ALL VA employees annually state, **“I will only use my access to VA computer systems and/or records for officially authorized and assigned duties.”** Official duties do not include accessing the information of relatives, friends or co-workers (regardless of permission from that party) unless the function has been specifically assigned.

Protection of Information

- **Types of information:**
 - **VA Sensitive Information.** For example: contract records, meeting minutes, research raw data
 - **Personally Identifiable Information (PII).** For example: names, SSNs, dates of birth, addresses
 - **Protected Health Information (PHI).** For example: medical records, prescription lists, lab results
- **How to protect:**
 - **Interoffice Mail:** When sending PII or PHI through interoffice mail, use Special Attention Privacy envelopes
 - **Email:** When emailing patient information, anything more than the patient's first initial of the last name and last 4 of the SSN needs to be encrypted

Unencrypted: A1234 left a message and is asking for a callback

Needs encrypted: A1234 left a message asking to reschedule his June 2nd appointment with Cardiology

Passwords

- Most systems use the PIV card to login.
- Must have at least 1 of each of the following:
 - Uppercase character
 - Lowercase character
 - Symbol
 - Number
- Must be at least 8 characters
- Changes every 90 days
- Not easily guessed
 - Not password
 - Avoid names of pets and relatives
 - Avoid birth dates



Personally Owned Devices and External Services

The following should not be connected to a VA computer, connected to the VA computer network, or used for VA job duties without written permission from the Area Manager and ISSO:

laptop

tablets, iPads

USB/flash/thumb drive

Dropbox

camera

Google Docs/Drive

smartphones

Blackboard

Saving Data

- Save everything to your:
 - U: User drive (My documents)
 - S: Services drive (Shared folders)
- Network drives are backed up daily so information can be recovered if lost
- Data saved on a network drive can be accessed from any VA computer, even at another VA
- Local computer hard drives are never backed up
- Anything saved on the Desktop will be backed up




Remote Access

- The VA network can be accessed remotely either with a VA laptop or personal computer when off-site
- Request must be submitted through self-service portal.
- This must be approved by your supervisor and Area Manager prior to being granted access.
- All network drives, email, and VistA can be accessed using this access.

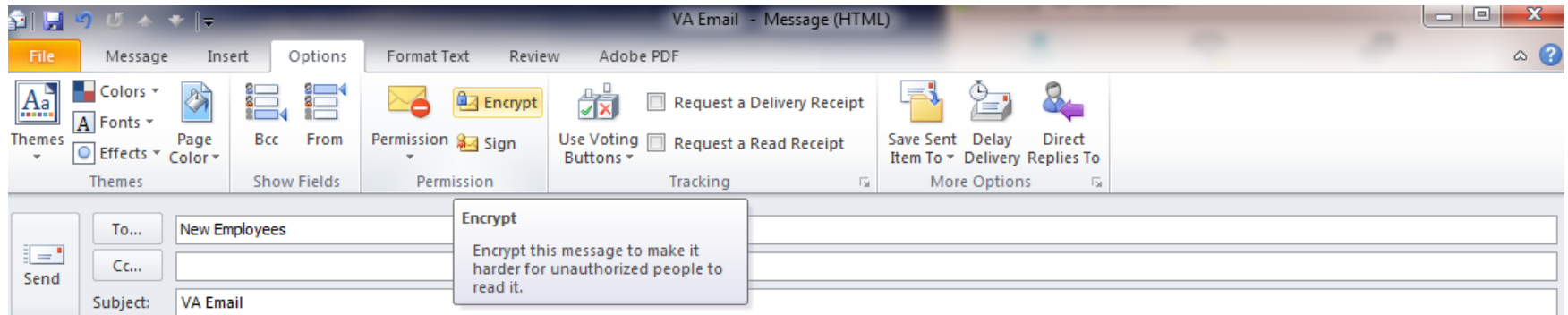


Past Audit Findings

- Unlocked computers
 -  + L
- Employees without proper ID
 - Visible, right side up
 - Information unobscured
- Staff not challenging those without IDs
 - If you see an unfamiliar person in your work area, question their reason for being there



VA Email

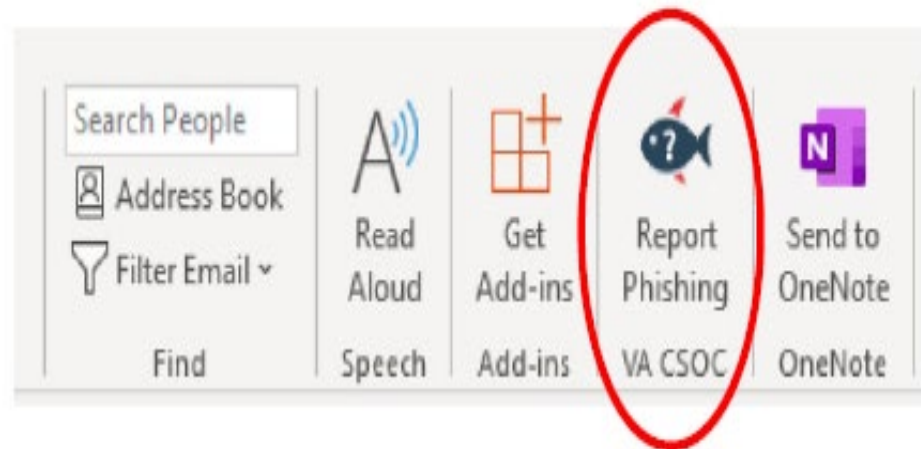


- Do not mix business with non-business.
- All emails can be requested through the Freedom of Information Act (FOIA).
 - Do not email anything you would not want the public to know.
 - Personal email cannot be requested under FOIA even if sent/received on a government computer.
- Do not email any sensitive or proprietary information to a non-VA email address.
- Do not open any suspicious emails from unknown non-VA email addresses.
- Be cautious opening emails with [EXTERNAL] in subject line.
- Do not put sensitive information in the subject line.

Report Phishing Attempts

The “**Report Phishing - CSOC**” button improves the employee experience and streamlines the reporting process to VA’s Cybersecurity Operations Center (CSOC). There are just three easy steps to report a phish:

- 1) Select the email in question, but don’t open it.
- 2) Click the “Report Phishing – CSOC” button located on the Outlook ribbon.
- 3) Click “Report.”



Limited Use of Resources Policy

- Employees are permitted to use VA computer systems for personal browsing at the following times:
 - During breaks
 - Before and/or after tour of duty
- No purchases should be made from a VA computer.
- Can never be used for a personal business.
- All Internet activity is monitored and logged.



Insider Threats

One of the biggest threats to the VA's data and information networks is the people who have the easiest access: Insiders

- Risks
 - An insider could use authorized access to harm information systems and VA sensitive information
 - An insider could become an involuntary threat by opening an attachment containing a virus that installs when opened
 - Establishing alternative methods for accessing the VA information system
- Prevention
 - Never share your account information
 - Do not open emails or attachments you aren't expecting
 - Use the access you've been given to the network only to perform your official duties

Reportable items

- All information security and privacy incidents must be reported to your supervisor and/or ISSO/PO IMMEDIATELY. Examples of reportable items are:
 - Lost/stolen PIV card, iPhone, iPad, Laptop, CD/DVD, VA USB drive, patient/employee records
 - Mis-mailed items
 - Unlocked computers
 - Unsecure patient/employee records
 - Auditory privacy concerns
 - Computer screen privacy
 - Virus attack
 - Suspicious email
 - Unencrypted emailing of sensitive information



- Often times the person affected by these types of incidents is provided credit monitoring protection or a HIPAA notification letter

Lessons Learned

- Employee who posted a staff selfie to Facebook with appointment list in background
- Nurse who accessed father's medical record
- Employee who allowed non-VA employee to use his ID badge for access
- Provider who left office unlocked with iPad, PIV card and patient information on desk
- Nurse took patient information home in tote bag
- Provider used Dropbox to transcribe patient notes

Q & A



Questions?